

Foto: Adobe Stock / Art_spiral/mit KI generiert

„Transparenz wird honoriert“

Was tun beim Cyberangriff? Ein Kommunikationsexperte aus Mainz gibt Tipps.

Die Zahl der Cyberangriffe steigt beständig. Datenklau, lahm gelegte Kassensysteme und Kommunikationskanäle, still stehende Produktionslinien, alles ist denkbar. Für Unternehmen stellt sich weniger die Frage, ob sie angegriffen werden, sondern wann – sagt Matthias Goldbeck, in Mainz ansässiger Partner beim Strategic Communication Consultant Network.

Seit der Corona-Zeit, als plötzlich Heimarbeit und Videokonferenzen boomten, ist dieser Trend verschärft zu beobachten. Aus der Pandemie lässt sich auch Goldbecks Grundregel ableiten: Vorbereitung schützt nicht vor Angriff, aber oft vor einem schweren Verlauf. Dabei geht es sowohl um IT-Sicherheit als auch um Verhaltensregeln – und die Kommunikation. Was im Fall eines erfolgreichen Cyberangriffs zu tun ist, sollte, so Goldbeck, Thema für den Vorstand sein – sowie für die gesamte Organisation und den Aufsichtsrat. Risikomanagement-Systeme ohne Cybersicherheit? Darf es nicht mehr geben. Der Experte rät, interdisziplinäre Krisenteams zusammenzustellen, mit IT-, Rechts-, Finanz-, Kommunikations-, Produktions- und Logistik-Fachleuten, sofern das Unternehmen entsprechend breit aufgestellt ist.

„Unternehmer sollten sich kritisch und ohne Vorbehalte überlegen, was im schlimmsten Fall passieren kann, und Pläne für den Fall des Falles erstellen, um dann nicht auf einem weißen Blatt Papier anzufangen“, sagt Goldbeck. Dazu zähle auch, auszuloten, in welchen Bereichen externe Beratung hinzugezogen werden soll, sei es in der Kommunikation, seien es spezialisierte Anbieter für Cybersicherheit, die teilweise auch Verhandlungen für Unternehmen mit den Cyberkriminelle führen. „Solche Spezialisten sichert man sich am besten schon vorher.“ Es gelte, Szenarien zu simulieren und Sprachregelungen vorzubereiten. Trainings mit Experten, die bereits praktische Erfahrung mit Angriffen gesammelt haben, seien am effektivsten. Nach außen hin zu mauern ist keine Lösung. Ein Schlüssel, neben der technischen Seite der Abwehr und Problembehebung, ist für



Foto: privat

Matthias Goldbeck

Goldbeck die Kommunikation, intern wie extern: „Kommunikation gehört an den Tisch, an dem entschieden wird, von Anfang an." Nach außen hin zu mauern aus Sorge, dass die Reputation darunter leidet, angegriffen worden zu sein, hält Goldbeck für verfehlt: „Sie sind hier das Opfer, nicht der Täter. So ist es auch in der Öffentlichkeit. Probleme bekommen Sie dann, wenn Sie Dinge unter der Decke halten, Kunden und Mitarbeiter nicht ausreichend informieren. Transparenz wird honoriert. Niemand will sich vorwerfen lassen, Kunden und Mitarbeitern nicht die Möglichkeit gegeben zu haben, sich zu schützen."

Natürlich sollte nur kommuniziert werden, was bereits eine gesicherte Erkenntnis ist. Und es gibt gesetzliche Verpflichtungen, was wann den Datenschutzbehörden zu melden ist. „Zu informieren, wenn Daten bedroht sind, ist für mich eine Kardinalstugend", sagt Goldbeck. „Ab dem Zeitpunkt des Entdeckens des Angriffs läuft die Uhr." Es gelte, im Blick zu behalten, wie nun über das Unternehmen berichtet und, etwa in den Sozialen Medien, gesprochen wird. „Wer es schafft, vor die Welle zu kommen, behält die Deutungshoheit." Elementar sei auch, dass die Beschäftigten wissen, wie sie sich in der Öffentlichkeit und privat äußern dürfen: „Jeder braucht die wesentlichen Fakten und muss wissen, was er sagen kann und darf."

Gut möglich ist, dass im Falle eines Angriffs die üblichen Kommunikationskanäle nicht mehr funktionieren. Kommunikation ohne E-Mails, Telefon- und Videokonferenzsysteme oder das Intranet? Auch für diesen Fall müssen Funktionsfähigkeit und Informationsweitergabe gewährleistet sein, durch alternative Strukturen etwa über Messenger und private Adressen, die günstigstenfalls physisch vorliegen.

Alle Unternehmen sind, wie Goldbeck betont, gut beraten, ihr Personal in Sachen IT-Sicherheit zu schulen: keine unbekannten Anhänge oder zweifelhaften Mails öffnen, nicht auf Links klicken, die nicht definitiv verlässlich sind. Angriffsobjekt ist meist der Nutzer. Das beliebteste Geschäftsmodell der Kriminellen ist derzeit, Daten zu klauen und als Geiseln zu nutzen. Wer nicht will, dass sie im Darknet landen, soll Lösegeld zahlen, in Kryptowährung.

Auch diese Szenarien müssen durchdacht werden. Welche Daten sind kritisch, welche Zugeständnisse ist man bereit zu machen? „Man sollte sich vorab im Klaren sein, wie man auf mögliche Forderungen reagiert", sagt Goldbeck. Denn je besser vorbereitet und damit sicherer der Angegriffene in der Krisenbewältigung ist, desto geringer fallen die Schäden aus.

TORBEN SCHRÖDER, FREIER JOURNALIST

12 REGELN FÜR GUTE KRISENKOMMUNIKATION

1. Planen Sie für den Ausnahmefall
2. Üben, üben, üben
3. Kommunikation ist Kerndisziplin
4. Es gelten die Prinzipien der Krisenkommunikation
5. Monitoring für schnelles Handeln und Social Media „beherrschen"
6. Alternative Kommunikationsstrukturen etablieren
7. Interne Kommunikation ist Key
8. Aktiv und transparent nach außen kommunizieren
9. Eine Attacke darf nicht überraschen
10. Thema gehört regelmäßig auf die Tagesordnung
11. Zugriffsrechte als potenzielle Gefahrenstelle
12. Sichern von Kapazität und Kompetenz

IT MADE IN GERMANY -
GEMEINSAM FÜR DEN DEUTSCHEN MITTELSTAND

Die WORTMANN AG ist einer der größten unabhängigen IT-Hersteller Europas – **mit Sitz, Produktion und Support in Deutschland.** TERRA steht für zuverlässige Hardware mit exzellentem Service, optimiert für Windows 11 Pro – ideal für modernes, sicheres und leistungsstarkes Arbeiten.

Mit Microsoft 365 profitieren Sie zusätzlich von smarter Teamarbeit, flexiblen Tools und sicherem Cloud-Zugriff – perfekt abgestimmt auf unsere TERRA Geräte.

www.wortmann.de

terra
IT. MADE IN GERMANY.

Starke IT.
Starke Partner.
Starke Zukunft.



Microsoft 365

Händler finden

WORTMANN AG
IT. MADE IN GERMANY.